IoT Gateway Security Mechanism for Efficient Network Establishment using Blockchain Implementation

Rajesh Kumar Sharma[1], Ravi Singh Pippal[2]

[1, 2] *Department of Computer Science & Engineering,*
RKDF University Bhopal India,
rajeshsharma.ercs@gmail.com
ravesingh@gmail.com

***Abstract*: *With the progressive growth in the deployment of Internet of Things (IoT) devices, security and protection of the huge volume of IoT data transmission has become a remarkable issue. IoT is basically a type of heterogeneous network composed of several devices and protocols. In this paper, an IoT gateway security mechanism is proposed for efficient IoT network establishment using Blockchain technology as a most effective and potential security technique on the basis of hit rate, total system hit rate and average response time of the network. A low powered device through IoT gateway is simulated that is decentralized and employed with Blockchain implementation. Proposed model carries a series of IoT devices that wirelessly communicate with each other. A server-client model is applied to each IoT device to communicate for application process. The simulated results show the significance of Blockchain technology as compared to centralized network. This work can bring many significant applications in industrial process and business*.**

***Keywords*: Internet of Things, Blockchain, IoT Gateway, Security, IoT Network.**

(Article history: Received 7th January 2021 and accepted on 29th June 2021)

I. INTRODUCTION

The Internet of Things (IoT) connect the daily-life objects of physical world to the network based digital world using several devices by providing sensing, data accumulation, analysis for particular activity [1]. Modern smart home system is a special case in the Internet of Things where personal devices at home are connected to the global Internet where remote users can get device status and send command to devices. There are many smart end-devices such as power meter, temperature controller; security door camera, smart led lighting etc. are linked to the gateway of smart home which transmits data to the cloud-based server as an IoT back-end [2].

The Internet of Things (IoT) based smart homes are platforms which provide intelligent and comfortable living environment, where security is the primary deal [3]. Ultimately, the IoT based smart home contains different subsystems for comfort life style where smart sensing devices are connected to the Internet for monitoring, exchanging and managing information to build the intelligent home. The concealed security issues are observed gradually with the growth of IoT based smart homes [4, 5]. It is essential to fulfill all security measures such as physical security, database, information transmission and processing, and gateway security for smart homes. Finally, the objective is to provide confidentiality, integrity and authenticity. The IoT gateway basically provides a bridge between sensing device and cloud server through Internet. The sensing devices communicate directly to the IoT gateway. The intermediate gateway collects and transfers the sensed data to the cloud server [6].

IoT benefited many industrial applications and smart home devices that are connected to the IoT gateway to collaborate with other intelligent process and services. Security and privacy of gateway becomes serious challenge to conserve intelligent IoT activities and services [7]. Basically, the data collected by actuators and sensors are sent to the cloud server through the IoT gateway where data are analyzed remotely. The end-to-end privacy preservation of smart home data or user's personal data is required by providing IoT gateway level security [8].

IoT gateway as an access object, designed with a fully secure infrastructure can effectively enhance the protection level of smart home devices [9]. Not only smart home, there are plenty of IoT applications such as smart building, vehicle, industry, city infrastructure etc, where automated security solution is on demand. Among the several security methods, the Blockchain technology is perfectly appropriate for IoT gateway level security system to automate process,

exchange real-time secure data communication and transactions [10]. This paper concentrates on the security of the IoT gateway using Blockchain technology by which personal and smart home security can be provided.

A. *Internet of Things Layered Architecture*

To analyze security, the IoT architecture should also be analyzed; it primarily contains application, network, and perception layer, as presented in Fig 1.

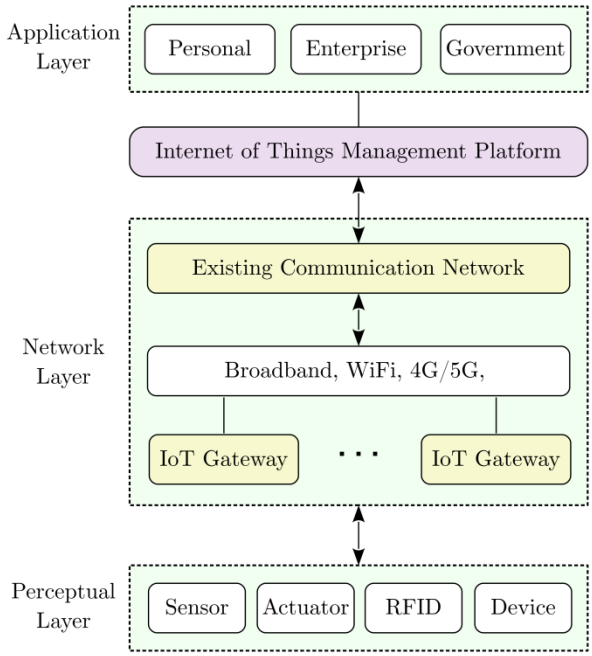

Fig. 1. Internet of Things Layered Architecture

For IoT security, the network layer takes the main responsibility. In the complex IoT network, the gateway in network layer receives data from perception layer to application layer for communication to the cloud server. Data travels into complex transmission environment through network layer of gateway which makes the security issue in IoT network [11].

B. *IoT Gateway Security Issues*

The home gateway is an intrinsic component of smart home, and it share and exchange information between several heterogeneous protocols with outside networks. IoT network can be integrated with several heterogeneous networks and there should be multi-interface gateway [12]. The gateway security system not only secures itself whereas it secures whole smart home components and appliances. So, gateway security is an essential and integral element of smart home system.

The IoT based smart home consists of the following security issues as presented in Fig 2.

- **Posing:** By supplying control commands, an intruder or attacker can pose himself as an end hosts to the gateway of smart home, also he can pose as a home gateway to pass fake data at the terminal host.
- **Replay:** There are two types of replay attack first is terminal host replay and second is home gateway replay.
- **Data Theft:** By tapping the line between through terminal host and smart home gateway, the data packets and information can be intercepted.
- **Virus Attack:** It is a very popular and common type of attack where the attacker inserts the virus into the data packet, and takes system resources.

DOS Attacks: The "denial-of-service (DOS)" attack and disrupt the network, and forbid the other user's access.

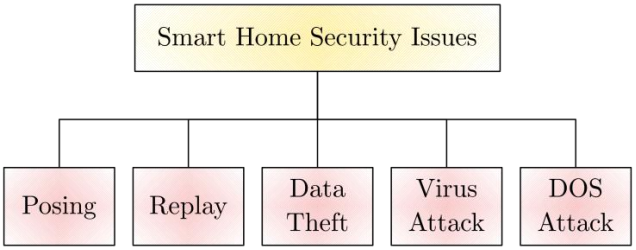

Fig. 2.Smart Home Security Issues

II. RELATED WORK

With the progressive evolution of IoT technology, it attempted and crucial role in the industrial transformation with economic and social development and its security system is much implicated content in several areas. The security in gateway of IoT network is the important step to secure whole network. This section presents various techniques for gateway level security of IoT network.

Jin *et al.* [13] proposed a micro service to secure IoT network by designing and implementing edge computing system. This secure micro service is deployed at localized network by edge gateway to offer data, device management and configuration as well as extra functionalities in the IoT network. Their proposed edge gateway computing management works as a hub which provides communication link between IoT devices and web clients. To support security services at edge gateway, the authentications and authorizations are provided by allowing the verified requests from local IoT network where gateway and devices are deployed.

Chang *et al.* [14] presented the IoT infrastructure which allows transferring the cryptographic signature creation process to its adjacent connected gateway device integrated with high speed GPU to minimize the load of sensing nodes. Generally, IoT gateway is connected with the multiple sensing nodes, so it is required getting sufficiently

higher signature creation rate by which huge amount of communication and data transmission can be handled. Their proposed IoT infrastructure exploits high speed GPU to boost up signature creation process and constitute the optimized implementation methods for RSA based cryptographic signature creation.

Cha *et al.* [15] proposed Blockchain integrated gateway to permit IoT service providers to give access users permissions based on privacy policy without replacing and changing the legacy of connected IoT devices. As a mediator the Blockchain based gateway is deployed between IoT devices and gateway where privacy policies of device and information can be obtained by the users. The users can access IoT devices through gateway and cannot access devices directly; consequently, the personal and sensitive data are prevented by gateway until privacy policies of IoT devices are accepted by the users. The preferences of users about privacy policies are stored as tamper-resistant data by Blockchain based gateway in the network.

Fraile *et al.* [16] presented "trustworthy industrial IoT gateway" using device driver security implementation applied in "virtual factory open operating system (vf-OS)" to interact physical IoT devices. They proposed a mechanism to reinforce resilience into the layer of device driver for realizing the system which can minimize the equipment casualties, damages or impairments by the consequences of intrusion or attack and it operations of device driver can be restored instantly and this process works based on fallback principle.

Kirupakar and Shalinie [17] proposed a new intelligent agent-based security framework for "Industrial Internet of Things (IIoT)" gateway for monitoring and recognizing several intrusions and security threats pointed to the IoT devices. This research also proposed a method for detection of cyber attack with low footprint and IIoT gateway is restricted to devices.

Xu and Wu [18] proposed a new "three-factor lightweight authentication method" for wireless sensor networks (WSNs) using multi-gateway structure. This method is securing in opposition to many intrusions and attacks verified by formal verification "ProVerif" as well as informal verification and also fulfill security characteristics.

Kim and Keum [19] proposed a trustworthy secure IoT gateway infrastructure which fabricates a trust domain for smart home to protect the IoT network from intrusion and malicious attack. Without making any modification in the network protocols of IoT devices, the trustworthy gateway infrastructure protects the IoT by altering the network address devices of smart home and device controlling server to an identifier which are recognized by local trust domain to connect non-trusted network.

Lee *et al.* [20] proposed tamper-proofed IoT gateway infrastructure based on Blockchain for the present IoT based smart home gateway system. The authentication, integrity and confidentiality related issues found in centralized gateway and heterogeneous IoT networks are provided by this infrastructure to build secure smart home. To solve the authentication and confidentiality issues occurred in gateway and IoT network, the secure hash algorithm 2 (SHA2) encryption technique is used. Moreover, the Blockchain is also helpful to confirm data integrity of gateway. The proposed network structure based on the Blockchain technology is evaluated with reference to the standard security measurement considering accuracy and security response.

Lucena *et al.* [21] analyzed the "gateway integrity checking protocol (GIP)" from the orientation of Intrusion Detection System. The proposed method uses a communication protocol which compiles data from IoT devices, to reply a request conveyed by the outer security agent. The reply is checked for integrity of data arrived in the server from the IoT gateway.

Kumar and Chouhan [22] proposed a "smart card based secure addressing and authentication (SCSAA)" method to defend the IoT network from intruders and attackers, and prepare trusted access into smart home applications and services. This method is generated by changing the standard IPv6 protocol. The method provides addressing of smart card using unique ID bits in IoT devices from which the server identifies each device uniquely without extra task. Moreover, the establishment of session key for identification of secrete keys enable the IoT network extra protective against various intrusions and attacks.

Gong *et al.* [23] presented a Blockchain based privacy protection framework for Internet of Things using proxy re-encryption and ring signature technique. In this framework, Blockchain based distributed storage system relieves the working burden of conventional centralized IoT network and the authorized users share this distributed data. The proxy re-encryption method included and established to secure the sharing of data between authorized user and service provider for ensuring data privacy. For transmitting ciphertext data, the proxy node works as an mediator which make this impossible to get the source address and link of sharing person's data. To provide effective protection of address information of sender's data and prevent deception by intermediary node, a ring signature method is applied that prevents this intermediary node from address of transaction parties.

Miloni *et al.* [24] presented "IEEE P1931.1 ROOF Standard", which provides potentiality into Internet of Things. There are many open challenges for trusted and decentralized IoT system to play crucial role for next steps

of future technology. This standard is need because artificial intelligence, Internet of Things and Blockchain will be completely autonomous system without any intervention and operation of human and in context-aware fashion. The "Real-Time Onsite Operations Facilitation (ROOF)" represents all of these important interplays.

For data security in IoT device, Kathayayani *et al.* [25] proposed "Hyperledger Fabric Blockchain". They provided fulfilled setup of ecosystem of IoT visualization including trusted as well as non-trusted entities. In this security-proof integrated system, data protection is kept preserved across this ecosystem. The performance results obtained in the analysis presents that regular functionalities and usefulness of the structure is reasonably under satisfactory position. Their proposed framework presents positive outcomes when the performance analysis is compared to the other framework. The ever-demanding requirements in IoT are provided by this system along with availability and security of data, backup and recovery, and scalability as a fundamental need.

Hossain *et al.* [26] added Ethereum (Blockchain based technique) into IoT devices for the concealment and security of the devices. Their proposed system can be applied to smarthomes as well as numerous types of IoT based projects. The proposed integration of Ethereum and IoT provide practical smart home application.

Zhang *et al.* [27] proposed a "Secure Method of Exchanging Resources in heterogeneous Internet of things (SMER)". To exchange resources for IoT devices in efficient, effective, secure, profitable manner, SMER system provides facilities for it. This research elaborates structure and a functional method of SMER system and developed a model based on operational process of SMER.

Chze *et al.* [28] presented "Cross-Layer Security Authentication Architecture (CLSA)" to enhance the security level of IoT devices for peer-to-peer (P2P) communications. Raspberry-Pi is integrated into this architecture that worked as secured gateway of IoT network. The outcomes presented secure peer-to-peer connection in the network of IoT devices.

III. III. Proposed System Model

With the successive proliferation of IoT based research, it provided extensive limit of applications in business, medical, education, industry and many other regions and also affected the modern lifestyle of people. Due to huge variety of IoT applications, the privacy and security problems have become highly crucial portion of the IoT network. To ensure and verify the regular activities of the system, any Internet of Things (IoT) based organizations essentially forever pay attention to their privacy and security. Blockchain technology, now a day, presents outstanding security schemes for networks and databases. The proposed IoT gateway security system based on Blockchain for efficient establishment of network is presented in Fig 3.

After designing and deploying the Blockchain based gateway and network, it is essential to deploy all edge computing IoT devices. The proposed process can be described according to the following steps:

- Initially, the local sample IoT devices are considered as independent synchronous devices.
- Using Gaussian model, a probability distribution model is developed to follow normal distribution and by adjusting all location and node degree in local network, maximum probability value for targeted function distribution is acquired.
- Using this value of maximum probability and distribution, the cluster of the IoT devices are created and center of the cluster is defined.
- Finally, the optimized result is obtained using iterative process of model components.

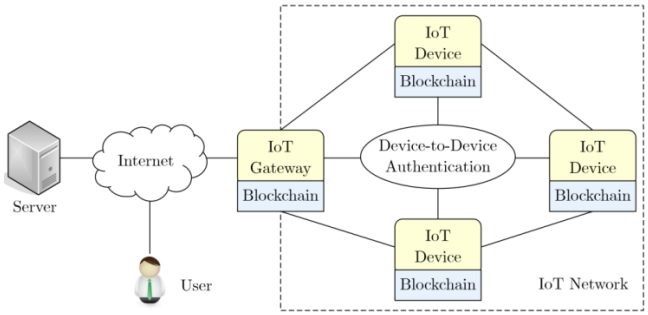

Fig. 3.Internet of Things Gateway Security

The distribution function of this process is presented by Equation 1:

$$f(x,\mu,\sigma) = \frac{1}{\sqrt{2\pi\sigma}} e^{-\frac{1}{2}(x-\mu)^2\sigma^{-2}} \qquad (1)$$

Where μ represents mean value, used for describing the centered location of the probability distribution; σ^2 represents variance, used to define the data density degree of IoT device. If this value is larger, then the distribution is more toward decentralized, and if the value is smaller, then it is the more centralized. The total summation of corresponding possibilities or probabilities is presented in Equation 2:

$$P(x_i,\mu,\sigma) = \sum_{j-1}^{K} \alpha_j \times f(x_i,\mu_j,\sigma_j) \qquad (2)$$

Where, α_j shows the weight of all the components and it requires to fulfil Equation 3:

$$\sum_{j-1}^{K} \alpha_j = 1, \quad 0 \leq \alpha_j \leq 1, \ \forall_j \in [1, K] \qquad (3)$$

On the bases of these equations, the average response time, hit rate and total system hit rate can be calculated, which can ensure that the requested work load of each device in the network covered by the processor of gateway will be insufficient in the condition for the maximum probability distribution for assuring its better working performance.

IV. IV. Result Analysis

This section presents the simulation result of proposed Blockchain based gateway security system. In this proposed network, it requires the data communication of node from nodes of other networks, where gateway keeps records of all transaction into Blockchain based distributed ledger system. For result assessment, hit rate, system hit rate, and average response time are considered as the featured parameters for analysis. Considering various storage size of IoT devices, the corresponding comparison of hit ratio for centralized network and Blockchain integrated gateway-based network is presented in Fig 4.

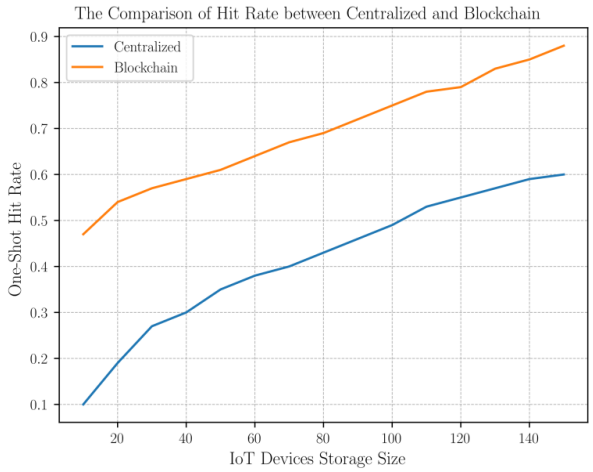

Fig. 4. The Comparison of Hit Rate for Centralized Network and Blockchain Integrated Gateway based Network

The corresponding comparison of system hit ratio for centralized network and Blockchain integrated gateway-based network is presented in Fig 5.

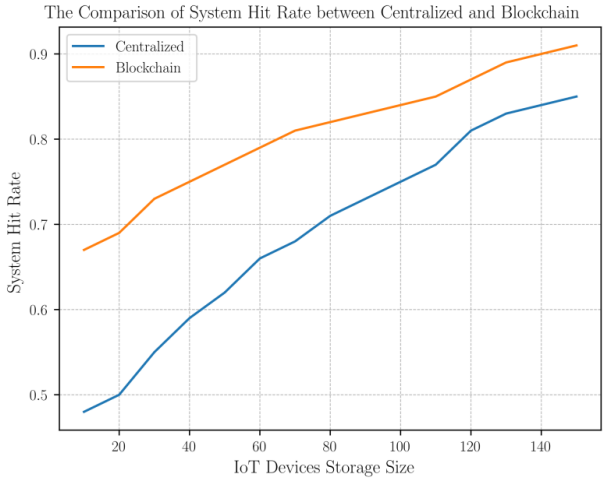

Fig. 5. The Comparison of System Hit Rate for Centralized Network and Blockchain Integrated Gateway based Network

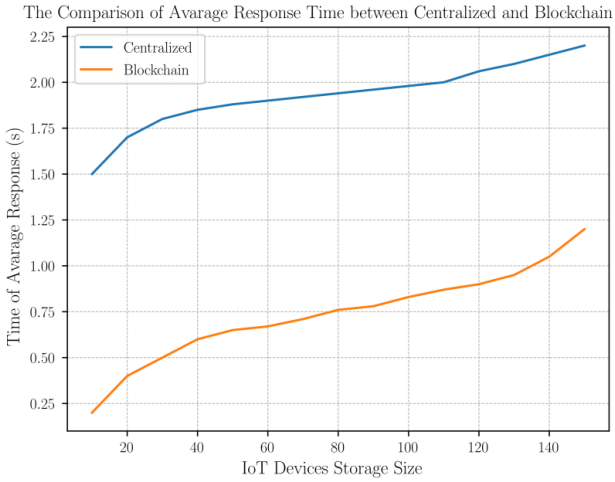

Fig. 6. The Comparison of Average Response Time for Centralized Network and Blockchain Integrated Gateway based Network

The comparative analysis of average response time for centralized network and Blockchain integrated gateway-based network is presented in Fig 6. With the increment of IoT devices storage size, the hit rate and the integrated system hit rate also increases. As presented in result from Fig 4 and 5, Blockchain based IoT gateway system shows higher one-shot hit rate as compared to centralized IoT network. Also, the average response time of Blockchain based gateway network is lower as compared to centralized system as presented in Fig 6, which means Blockchain-enabled gateway based decentralized IoT network not only secure as well as its responses significantly faster as

compared to centralized IoT network with the increment of storage size of IoT devices.

Finally, analyzing the throughput and security issues of the IoT nodes from the visual aspect of the privacy and security of the gateways and IoT devices, the high potential privacy risks in the network is comprehensible, so Blockchain based secure integrated system is required for gateway of the IoT network.

V. Conclusion and Future Work

With the endless progressive evolution of modern technologies, the IoT based application is very common and more widely, and countless IoT devices are connected to the heterogeneous network, so the privacy and security issues have become the big concern and challenge for researchers, technicians and relevant experts. The network of IoT devices with gateway are analyzed, on the basis of hit rate, total system hit rate of network and average response time are simulated and optimized for centralized and Blockchain-based distributed system. From the result analysis, it is clear that Blockchain provides high security as well as high responsive network.

However, in this research work, only the privacy and security of gateways and IoT devices are analyzed, whereas the security and integrity of sensor nodes, clouds servers, and other controllers are not analyzed, that will be deliberated in the future work in more detail using more comprehensive analysis. Analysis of IoT devices and gateway security are of high significance to expand the application area of Internet of Things. It also allows for many estimations for the further work of IoT based computation, security analysis and encourages the growth of the IoT network

References

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010.doi: https://doi.org/10.1016/j.comnet.2010.05.010

[2] D. Chattopadhyay, A. Samantaray, and A. Datta, "Device micro agent for IoT home gateway: A lightweight plug-n-play architecture," SIGBED Rev., vol. 15, no. 2, pp. 16–23, Jun. 2018. doi: https://doi.org/10.1145/3231535.3231537

[3] F. Li, Z. Wan, X. Xiong, and J. Tan, "Research on sensor gateway terminal security mechanism of smart home based on IoT," in Internet of Things, Y. Wang and X. Zhang, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 415–422. doi: https://doi.org/10.1007/978-3-642-32427-7_58

[4] S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, "I-SHSS: An IoT based smart home security system," in Advanced Multimedia and Ubiquitous Engineering, J. J. J. H. Park, S.-C. Chen, and K.-K. Raymond Choo, Eds. Singapore: Springer Singapore, 2017, pp. 303–306. doi: https://doi.org/10.1007/978-981-10-5041-1_51

[5] U. Erlingsson, B. Livshits, and Y. Xie, "End-to-end web application security," in Proceedings of the 11th USENIX Workshop on Hot Topics in Operating Systems, ser. HOTOS'07. USA: USENIX Association, 2007.

[6] F. Balali, J. Nouri, A. Nasiri, and T. Zhao, IoT Platform: Smart Devices, Gateways, and Communication Networks. Cham: Springer International Publishing, 2020, pp. 67–77. doi: https://doi.org/10.1007/978-3-030-35930-0 5

[7] Y. Lee, W. Lee, G. Shin, and K. Kim, "Assessing the impact of dos attacks on IoT gateway," in Advanced Multimedia and Ubiquitous Engineering, J. J. J. H. Park, S.-C. Chen, and K.-K. Raymond Choo, Eds. Singapore: Springer Singapore, 2017, pp. 252–257. doi: https://doi.org/10.1007/978-981-10-5041-1_43

[8] F. Loukil, C. Ghedira-Guegan, K. Boukadi, and A. N. Benharkat, "Semantic IoT gateway: Towards automated generation of privacy-preserving smart contracts in the Internet of Things," in On the Move to Meaningful Internet Systems. OTM 2018 Conferences, H. Panetto, C. Debruyne, H. A. Proper, C. A. Ardagna, D. Roman, and R. Meersman, Eds. Cham: Springer International Publishing, 2018, pp.207–225. doi: https://doi.org/10.1007/978-3-030-02610-3 12

[9] J. Fan, Z. Wang, and C. Li, "Design and implementation of IoT gateway security system," in 2019 International Conference on Artificial Intelligence and Advanced Manufacturing (AIAM),2019, pp. 156–162. doi:https://doi.org/10.1109/AIAM48774.2019.00039

[10] H.-C. Chen, "A trust evaluation gateway for distributed Blockchain IoT network," in Wireless Internet, J.-L. Chen, A.-C. Pang, D.-J. Deng, and C.-C. Lin, Eds. Cham:Springer International Publishing, 2019, pp. 156–162. doi:https://doi.org/10.1007/978-3-030-06158-6_16

[11] Z. Lv, "Security of internet of things edge devices," Software: Practice and Experience, pp. 1–11, Feb 2020. doi:https://doi.org/10.1002/spe.2806

[12] Z.-y. Bai, C.-H. Kuo, and T.-C. Wang, "Design and implementation of an IoT multi-interface gateway for establishing a digital art interactive system," International Journal of Ad Hoc and Ubiquitous Computing, vol. 21, no. 3, pp. 157–170, 2016. doi:https://doi.org/10.1504/IJAHUC.2016.075376

[13] W. Jin, R. Xu, T. You, Y. G. Hong, and D. Kim, "Secure edge computing management based on independent micro services providers for gateway-centric IoT networks," IEEE Access, vol. 8, pp. 187 975–187 990, 2020. doi:https://doi.org/10.1109/ACCESS.2020.3030297

[14] C. Chang, W. Lee, Y. Liu, B. Goi, and R. C. .Phan, "Signature gateway: Offloading signature generation to IoT gateway accelerated by GPU," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4448–4461, 2019. doi:https://doi.org/10.1109/JIOT.2018.2881425

[15] S. Cha, J. Chen, C. Su, and K. Yeh, "A Blockchain connected gateway for BLE-based devices in the Internet of Things," IEEE Access, vol. 6, pp. 24 639–24 649, 2018. doi:https://doi.org/10.1109/ACCESS.2018.2799942

[16] F. Fraile, T. Tagawa, R. Poler, and A. Ortiz, "Trustworthy industrial IoT gateways for interoperability platforms and ecosystems," IEEE Internet of Things Journal, vol. 5, no. 6,pp. 4506–4514, 2018. doi: https://doi.org/10.1109/JIOT.2018.2832041

[17] J. Kirupakar and S. M. Shalinie, "Situation aware intrusion detection system design for industrial IoT gateways," in2019 International Conference on Computational Intelligence in Data Science (ICCIDS), 2019, pp. 1–6. doi: https://doi.org/10.1109/ICCIDS.2019.8862038

[18] L. Xu and F. Wu, "A lightweight authentication scheme for multi-gateway wireless sensor networks under IoT conception," Arabian Journal for Science and Engineering, vol. 44,no. 4, pp. 3977–3993, Apr 2019. doi: https://doi.org/10.1007/s13369-019-03752-7

[19] E. Kim and C. Keum, "Trustworthy gateway system providing IoT trust domain of smart home," in 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN), 2017,pp. 551–553. doi: https://doi.org/10.1109/ICUFN.2017.7993848

[20] Y. Lee, S. Rathore, J. H. Park, and J. H. Park, "A Blockchain based smart home gateway architecture for preventing data forgery,"

Human-centric Computing and Information Sciences, vol. 10, no. 1, pp. 1–14, Mar 2020. doi:https://doi.org/10.1186/s13673-020-0214-5

[21] M. Mart´ınez de Lucena, R. M. Scheffel, and A. A. Frohlich, "An analysis of the gateway integrity checking protocol from the perspective of intrusion detection systems, "Design Automation for Embedded Systems, Sep 2020. doi:https://doi.org/10.1007/s10617-020-09240-8

[22] P. Kumar and L. Chouhan, "A secure authentication scheme for IoT application in smart home," Peer-to-Peer Networkingand Applications, Aug 2020. doi: https://doi.org/10.1007/s12083-020-00973-8

[23] J. Gong, Y. Mei, F. Xiang, H. Hong, Y. Sun, and Z. Sun, "A data privacy protection scheme for internet of things based on Blockchain," Transactions on Emerging Telecommunications Technologies, p. e4010.doi: https://doi.org/10.1002/ett.4010

[24] A. Meloni, S. Madanapalli, S. K. Divakaran, S. F. Browdy, A. Paranthaman, A. Jasti, N. Krishna, and D. Kumar, "Exploiting the IoT potential of Blockchain in the IEEE p1931.1 roof standard," IEEE Communications Standards Magazine, vol. 2, no. 3, pp. 38–44, Sept 2018. doi:https://doi.org/10.1109/MCOMSTD.2018.1800019

[25] N. Kathayayani, J. K. Murthy, and V. N. Naik, "Hyperledger fabric Blockchain for data security in IoT devices," International Journal of Recent Technology and Engineering (IJRTE),vol. 9, no. 1, pp. 2571–2577, May 2020. doi: https://doi.org/10.35940/ijrte.A3040.059120

[26] M. S. Hossain, S. Waheed, Z. Rahman, S. A. Shezan, and M. M. Hossain, "Blockchain for the security of internet of things: A smart home use case using Ethereum, "International Journal of Recent Technology and Engineering(IJRTE), vol. 8, no. 5, pp. 4701–4608, Jan 2020.doi:https://doi.org/10.35940/ijrte.E6861.018520

[27] Y. Zhang, Y. Han, and J. Wen, "SMER: a secure methodof exchanging resources in heterogeneous Internet of Things,"Frontiers of Computer Science, vol. 13, no. 6, pp. 1198–1209,Dec 2019. doi: https://doi.org/10.1007/s11704-018-6524-3

[28] P. L. R. Chze, K. S. Leong, A. K. Wee, E. Sim, K. E.May, Y. J. Jie, and H. S. Wing, "Secured IoT gateway for smart nation applications," in 2018 14th International WirelessCommunications Mobile Computing Conference (IWCMC),2018, pp. 1065–1068. doi: https://doi.org/10.1109/IWCMC.2018.8450362

[29] R.K. Sharma, R.S. Pippal, "Malicious Attack and Intrusion Prevention in IoT Network Using Blockchain Based Security Analysis," in 2020 12th IEEE International Conference on Computational Intelligence and Communication Networks (CICN 2020), doi: https://doi.org/10.1109/CICN49253.2020.9242610

AUTHOR PROFILE

Rajesh Kumar Sharma
RKDF University Bhopal,
Associate Professor ,
12 year Academic Experience.
Department :- Computer Science and Engineering,
Area of Specialization(Internet of things, Blockchain)
Publication :- 05

Dr. Ravi Singh Pippal
RKDF University Bhopal,
Associate Professor ,
Dean Engineering and Technology
15 year Academic Experience.
Department :- Computer Science and Engineering,
Publication :- 88